

## REMARKS

In response to the Office Action, Claims 1, 20-22, 24, and 38-40 are amended. Claims 2, 6, 7, 27, and 28 were previously canceled. Claims 1, 3-5, 8-26 and 29-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

### **I. Claims Rejected Under 35 U.S.C. §103**

A. Claims 1, 3-5, 8-22, 24-26 and 29-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"), in view of Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, 1997, pages 234-237 ("Menezes") and further in view of *Simple Network Authenticating Key Exchange* ("SNAKE").

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Claim 1, as amended, includes the elements of

generating, at the first entity, a first secret  $S_B$  using a combining function  $f_B$  on at least a first password  $P_B$ , the first public key  $M_B$ , and the second public key  $M_A$ ;

generating, at the first entity, a first session key  $K_B$ , the first session key  $K_B$  being different from the first secret  $S_B$ , both the first session key  $K_B$  and the first secret  $S_B$  being computed from the second public key  $M_A$ ;

encrypting, at the first entity, a first random nonce  $N_B$  with the first session key  $K_B$  or the first secret  $S_B$  to obtain a first encrypted result, the first random nonce  $N_B$  being unrelated to both  $K_B$  and  $S_B$ ;

encrypting, at the first entity, the first encrypted result with the other one of the first session key  $K_B$  or the first secret  $S_B$  to obtain an encrypted random nonce

(emphasis added). Applicants submit that Vogelesang in view of Menezes and further in view of SNAKE does not teach or suggest encrypting a random nonce  $N_B$  using a first session key  $K_B$  and a first secret  $S_B$ , wherein  $K_B$  is different from  $S_B$ , both  $K_B$  and  $S_B$  are computed from the second public key  $M_A$ , and both  $K_B$  and  $S_B$  are unrelated to the random nonce  $N_B$ .

Vogeleang discloses a cryptographic system in which signals between two participants are encrypted with one encryption key. The Examiner recognizes that Vogeleang does not disclose encryption with two encryption keys, but relies on Menezes to disclose double encryption. Menezes discloses encrypting a message with two encryption keys. However, Menezes does not disclose the specific characteristics of the two encrypted keys recited in Claim 1. Specifically, Menezes does not disclose the two encryption keys being different, both computed from the second public key, and both unrelated to the message to be encrypted.

SNAKE is relied on to disclose the use of a combining function  $f_B$  on at least a first password  $P_B$ , the first public key  $M_B$ , and the second public key  $M_A$  to generate one of the encryption keys (the recited  $S_B$ ). SNAKE discloses a key exchange protocol in which a random number ( $S$  or  $R$ ) is encrypted with a key  $K$  before transmission to another party (page 1). SNAKE discloses that  $K$  is generated using a hash function ( $H$ ) applied on at least a pass phrase ( $P$ ) and two public messages (Message1, Message2). Message1 and Message2 are formed by the random numbers  $R$  and  $S$ , respectively, concatenated with other elements. As a result, the encryption key  $K$  is derived from the same random number that the encryption key  $K$  encrypts. Thus, the encryption key  $K$  is not unrelated to the random number that it encrypts. Thus, SNAKE does not teach or suggest the recited first secret  $S_B$ . None of the cited references teach or suggest encrypting a random nonce with two encryption keys, the two encryption keys being different, both computed from the second public key, and both unrelated to the random nonce.

Moreover, Applicants submit that the proposed combination of the cited references is based on impermissible hindsight construction. Each of the cited references discloses well-known cryptographic operations. However, the cited references do not teach or suggest that these cryptographic operations can be modified and combined to produce the claimed invention. The encryption key ( $S$ ) of Vogeleang is used to encrypt a private message (e.g., a private signal  $D$  at col. 16, line 50-55). The encryption key ( $K$ ) of SNAKE is used to encrypt a public message (e.g.,  $S$  or  $R$ , which is a message transmitted in the clear). There is no teaching or suggestion in these references to combine an encryption key for a private message with another encryption key for a public message. Thus, the proposed combination is inapposite.

For at least the foregoing reasons, the cited references do not teach or suggest each of the elements of Claim 1. Thus, Claim 1 is non-obvious over the cited references.

Claims 3-5 and 8-19 depend from Claim 1 and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 1, these claims are non-obvious over the cited references. Analogous discussions apply to independent Claims 20-22, 24, and 38-40, which are amended to include similar limitations. Claims 25, 26, 29-37 and 41 depend from Claims 24 and 40, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above, these claims are non-obvious over the cited references.

Accordingly, reconsideration and withdrawal of the §103 rejection of Claims 1, 3-5, 8-22, 24-26 and 29-41 are respectfully requested.

B. Claim 23 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Vogelesang in view of Menezes and further in view of SNAKE.

Claim 23 depends from Claim 22 and incorporates the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 22, the cited references do not teach or suggest each of the elements of Claim 23.

Accordingly, reconsideration and withdrawal of the §103 rejection of Claim 23 are requested.

**CONCLUSION**

In view of the foregoing, it is believed that all claims are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

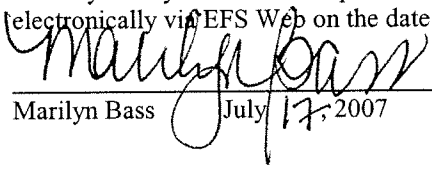
Dated: July 17, 2007

1279 Oakmead Parkway  
Sunnyvale, CA 94085-4040  
(310) 207-3800

  
\_\_\_\_\_  
Jonathan S. Miller, Reg. No. 48,534

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below

  
\_\_\_\_\_  
Marilyn Bass July 17, 2007